

ADVISORY: U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS ISSUES ITS ANNUAL REPORT TO CONGRESS ON BREACHES OF UNSECURED PROTECTED INFORMATION

By: *Kristen Blanchette*
Email: kblanchette@devinemillimet.com
Phone: 603.695.8572

JANUARY 30, 2012

In the fall of 2011, the U.S. Department of Health and Human Services (“HHS”) Office for Civil Rights (“OCR”) provided a report to Congress on health information breaches from September 2009 through 2010. A report for 2011 has not yet been released. According to the report, nearly 7.9 million Americans were affected by almost 30,800 health information breaches—207 of the breaches in 2010 involved more than 500 or more individuals.

This annual report to Congress is mandated by the Health Information Technology for Economic and Clinical Health (“HITECH”). HITECH, enacted in 2009, made significant changes to the HIPAA Privacy and Security Rules. One of the most important changes was the requirement that hospitals notify patients of a “breach” of their “unsecured” protected health information (“PHI”). The HITECH Act divides breaches into two categories: breaches involving less than 500 individuals (“Small Breaches”) and breaches involving 500 or more individuals (“Large Breaches”). A covered entity must report a Large Breach to the Secretary of HHS (via OCR) at the same time the covered entity notifies the affected individuals (without unreasonable delay and no more than sixty days following discovery of the breach, subject to limited exceptions). Information about breaches involving 500 or more individuals is available at, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html> Reports of Small Breaches are due to OCR no later than sixty days following the end of the calendar year in which the breach occurred, although a covered entity may report a Small Breach at any time prior to that date.

The five main causes of these Large Breaches in 2010 were, in order of frequency: (1) theft; (2) loss of electronic media or paper records containing protected health information; (3) unauthorized access to, use or disclosure of PHI; (4) human error; (5) and improper disposal.

Data breaches reported between September and December 2009

Office Locations:

111 Amherst Street
Manchester, NH 03101
T 603.669.1000
F 603.669.8547

43 North Main Street
Concord, NH 03301
T 603.226.1000
F 603.226.1001

DEVINEMILLIMET.COM

HEALTHCARE@DEVINEMILLIMET.COM

identified the same first four causes as in 2010 but did not include improper disposal. In the three months of 2009 and in 2010, theft was the most common cause.

We expect that 2011's report will continue to show theft as the most common cause for large data breaches. In fact, the largest reported theft to date, affecting 1.9 million people, occurred in 2011. In this particular breach, a business associate providing information services to a hospital system left a vehicle unlocked and unattended and a person stole electronic files containing PHI. See New York City Health and Hospitals Corporation, HHC Reports Theft of Personal Health Information (Feb. 11, 2011), at www.nyc.gov/html/hhc/html/pressroom/pr-20110211-data-theft.shtml.

What can entities do to mitigate or prevent these breaches?

- Improve physical security by installing new security systems or by relocating equipment or records to a more secure area.
- Adopt encryption technologies.
- Change passwords.
- Provide extensive training and retraining of employees that handle protected health information.
- Revise policies and procedures.
- Impose sanctions on workforce members who violate policies and procedures regarding protect health information including unauthorized access.
- Collaborate with others in health care (include those that are outside of compliance, i.e. legal/outside counsel, computer forensics).

The Devine, Millimet & Branch Healthcare Practice offers this free periodic E-Mail Alert service to provide information on recent healthcare developments in statutory, regulatory and case law, and decisions. If you have any questions about this e-mail, or if you know of anyone else who may be interested in receiving these alerts, please send us an e-mail at healthcare@devinemillimet.com.